UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. JOSEPH KLINE, Defendant.	CASE NO. 15cr0503-WQH ORDER

HAYES, Judge:

The matters before the Court are the motion to dismiss information (ECF No. 27-1), and the motion to suppress fruit of unlawful search. (ECF No. 27-2).

I. Procedural Background

Defendant Joseph Kline is charged in an information with distribution of visual depictions of digital and computer images which contain materials the production of which involved the use of a minor engaging in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2), and possession of visual depictions of digital and computer images which contain materials the production of which involved the use of a minor engaging in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(4)(B).

On May 18, 2015, Defendant filed a motion to dismiss the information on the grounds that 18 U.S.C. § 2252(a) violates the First Amendment of the United States Constitution, and a motion to suppress fruit of unlawful searches on the grounds that

the Government obtained his IP address through a warrantless search.[1] On May 27, 2015, the United States filed a response. On July 29, 2015, the Court held an evidentiary hearing at which the Government presented the testimony of Special Agent Edward Coderes, employed by the Department of Homeland Security, Homeland Security Investigations.

II. Motion to Dismiss Information

Section 2252 prohibits an individual from knowingly distributing or possessing any visual depiction "of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2252(a). "'Minor' means any person under the age of eighteen years." 18 U.S.C. § 2256(1).

Defendant contends that 18 U.S.C. § 2252(a) is overbroad on its face because the definition of "minor" in 18 U.S.C. § 2256(1) includes 16- and 17-year-olds. Defendant asserts that Congressional reasoning for criminalizing the distribution or possession of visual depictions of 16- and 17-year-olds engaged in sexually explicit conduct conflicts with First Amendment jurisprudence in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002). Defendant contends that the federal age of consent is 16 and that § 2252(a) criminalizes a substantial amount of protected speech (conduct) involving 16- and 17-year-olds.

The Government contends that the United States Supreme Court determined in *United States v. X-Citement Video, Inc.*, 513 U.S. 64 (1994) that § 2252(a) is not constitutionally overbroad on the grounds that §2256 "makes the age of majority 18, rather than 16." *Id*. at 79. The Government contends that some instances in which the law treats 16- and 17-year-olds as adults does not require "adult treatment of the older minors" in child pornography statutes. (ECF No. 28 at 6).

In *New York v. Ferber*, 458 U.S. 747 (1982), a New York statute prohibiting

[1]Defendant has withdrawn the motion to suppress evidence for a *Gantt* violation (ECF No. 27-3), and the parties agree that the motion to suppress statements (ECF No. 27-4) is moot on the grounds that the Government has represented it will not use the statements in its case-in-chief.

persons from knowingly promoting a sexual performance by a minor up to the age of 16 was upheld as constitutional. The Supreme Court concluded that the prohibition was not overbroad because the proscribed activities were "intrinsically related to the sexual abuse of children." *Id.* at 759. The Supreme Court explained that "the materials produced are a permanent record of the children's participation and the harm to the child is exacerbated by their circulation." *Id.* The Supreme Court stated that "the conduct to be prohibited must be adequately defined by the applicable . . . law." *Id.* at 764. The Supreme Court concluded that "the nature of the harm to be combated requires that the [offense] be limited to works that *visually* depict sexual conduct by children below a specified age."[2] *Id.* The Supreme Court found the New York statute within these parameters and concluded that "it is permissible to consider these materials as without the protection of the First Amendment." *Id.*

In 1984, Congress amended the definition of minor for the purpose of the federal pornography laws increasing definition of minor from a person under the age of 16 to a person under the age of 18. Congressional records include the following comment:

> The Committee concluded that the age of children encompassed by the act should be increased from 16 to 18 years. The prosecution for distribution are (sic) most often solely on the pornography which is the subject of the offense; the children cannot be located. Based on the pictures alone, the prosecution must show that the child is under the age of 16. This is extremely difficult once the child shows any sign of puberty. Raising the age to 18 would facilitate the prosecution of child pornography cases and raise the effective age of protection from these practices, probably not to 18 years of age, but perhaps to 16.

H.R.Rep. No. 98-536, 1983 WL 25391 (November 10, 1983).

In *X-Citement Video, Inc.*, the United States Supreme Court upheld the constitutionality of § 2252 "conclud[ing] that the term 'knowingly' in § 2252 extends both to the sexually explicit nature of the material and to the age of the performers." 513 U.S. at 78. The Supreme Court further stated:

As an alternative grounds for upholding the reversal of their convictions,

---

[2] The Supreme Court noted that "sixteen states define a child as under age 18. Four States define a child as under 17 years old. The federal law and 16 States, including New York, define a child as a person under age 16." 458 U.S. at 764 n. 17.

> respondents reiterate their constitutional challenge to 18 U.S.C. § 2256. These claims were not encompassed in the question on which this Court granted certiorari, but a prevailing party, without cross-petitioning, is "entitled under our precedents to urge any grounds which would lend support to the judgment below." *Dayton Bd. of Ed. v. Brinkman*, 433 U.S. 406, 419, 97 S.Ct. 2766, 2775, 53 L.Ed.2d 851 (1977). Respondents argue that § 2256 is unconstitutionally vague and overbroad because it makes the age of majority 18, rather than 16 as did the New York statute upheld in *New York v. Ferber*, *supra*, and because Congress replaced the term "lewd" with the term "lascivious" in defining illegal exhibition of the genitals of children. We regard these claims as insubstantial, and reject them for the reasons stated by the Court of Appeals in its opinion in this case.

513 U.S. at 78-79. The Court of Appeals had stated, "we would not lightly hold that the Constitution disables our society from protecting those members it traditionally considered to be entitled to special protections - minors." *U.S. v. X-Citement Video, Inc.*, 982 F.2d 1285, 1288 (9th Cir. 1992), *rev'd on other grounds*, 513 U.S. 64 (1994). The Court of Appeals recognized a "series of Supreme Court cases that permit 'adult' treatment of 16- and 17-year-olds" noting that these "Supreme Court cases . . . merely permit, rather than require, adult treatment of 16- and 17-year-olds." 982 F.2d at 1288. The Court of Appeals concluded that the Supreme Court cases "indicate nothing about the substantiality (or lack thereof) of the overbreadth of section 2256" and concluded that the defendant's arguments are "far from sufficient to overcome the presumption against invalidating a statute on its face for overbreadth." *Id.*

In *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002), a trade association of businesses brought a pre-enforcement freedom of speech challenge to extending the federal prohibition against child pornography to sexually explicit images that appear to depict minors but were produced without using any real children. The Supreme Court examined a provision of the Child Pornography Protection Act (CPPA) enacted in 1996 which extended the federal prohibition against child pornography to any visual depiction that "is, or appears to be, of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8)(B). This prohibition captured "a range of depictions, sometimes called 'virtual child pornography.'" *Id*. at 256. The Supreme Court explained,

> As a general principle, the First Amendment bars the government from dictating what we see or read or speak or hear. The freedom of speech has

> its limits; it does not embrace certain categories of speech, including defamation, incitement, obscenity, and pornography produced with real children.

535 U.S. at 245-46. The Supreme Court explained that "these categories may be prohibited without violating the First Amendment" but concluded that "none of them includes the [virtual child pornography] prohibited by the CPPA." *Id*. at 246.

The Supreme Court in *Ashcroft* recognized that "[t]he CPPA . . . extends to images that appear to depict a minor engaging in sexually explicit activity without regard to the *Miller*[3] requirements" . . . prohibit[ing] speech despite its serious literary, artistic, political, or scientific value." *Id*. at 246. The Supreme Court then turned to its reason for excluding child pornography from the protection of the First Amendment in *Ferber*. The Supreme Court stated, "Where the images are themselves the product of child sexual abuse, *Ferber* recognized that the State had an interest in stamping it out without regard to any judgment about its content." *Id*. at 249. The Supreme Court concluded, "In contrast to the speech in *Ferber*, speech that itself is the record of sexual abuse, the CPPA prohibits speech that records no crime and creates no victims by its production. Virtual child pornography is not 'instrinsically related' to the sexual abuse of children, as were the materials in *Ferber*." *Id*. at 250. The Supreme Court concluded that "virtual child pornography" produced without children "covers materials beyond the categories recognized in *Ferber* and *Miller*, and the reasons the Government offers have no justification in our precedents or in the law of the First Amendment." *Id.* at 256. Because § 2256(8)(B) abridged the freedom to engage in a substantial amount of lawful speech, the Court found the provision overbroad and unconstitutional.

In this case, the prohibition in § 2252(a) is directed to knowingly possessing or distributing a visual depiction of sexually explicit conduct of actual minors below the specified age of 18. Defendant asserts that the statute is unconstitutional because it

---

[3] "Under *Miller v. California*, 413 U.S. 15, 93 S.Ct. 2607, 37 L.Ed.2d 419 (1973), the Government must prove that the work, taken as a whole, appeals to the prurient interest, is patently offensive in light of community standards, and lacks serious literary, artistic, political, or scientific value." *Ashcroft*, 535 U.S. at 246.

includes "all sexually explicit depictions of 16- and 17-year-olds, even those with literary value." (ECF No. 27-1 at 6). This specific challenge to the inclusion of 16- and 17-year-olds in § 2256 was rejected by the Supreme Court in *X-Citement Video*. *See* 513 U.S. at 78-79 ("Respondents argue that § 2256 is unconstitutionally vague and overbroad because it makes the age of majority 18, rather than 16 as did the New York statute upheld in *New York v. Ferber*, *supra*, ... We regard these claims as insubstantial, and reject them."). The holding in *Ashcroft v. Free Speech Coalition*, invalidating a federal prohibition against virtual child pornography on the grounds that no minor is harmed by the production is not contrary to the decision of the Supreme Court to uphold a challenge to the majority age of 18.[4] This district court follows the holding of the Supreme Court in *X-Citement Video* that §2256 is not "unconstitutionally vague and overbroad because it makes the age of majority 18, rather than 16." *X-Citement Video*, 513 U.S. at 78.

Defendant's motion to dismiss is denied.

III. Motion to Suppress Fruit of Unlawful Searches

On December 5, 2013, Special Agent Coderes was investigating suspected child pornography on the Gnutella network. Gnutella is an internet-based file sharing network that allows users who have downloaded peer-to-peer software to make certain files available for anyone on the internet who has also downloaded the peer-to-peer software.[5]

The agent testified that he used a software program called Child Protective System (CPS) to look for known images of child pornography on the Gnutella network. The agent testified that the CPS software program had a geo-locate feature designed to limit the network search to the area of his investigative authority. The agent testified

---

[4] In *Ashcroft*, the Supreme Court recognized that "images [of sexually explicit activity] are prohibited so long as the persons appear to be under 18 years of age. *This is higher than the legal age for marriage in many States, as well as the age at which persons may consent to sexual relations.*" 535 U.S. at 246 (emphasis added).

[5] A peer-to-peer network allows files to be shared with selected users.

that the CPS software searches for known hashtags for confirmed child pornography images and provides law enforcement with the Internet Protocol (IP) address and sometimes the global unique identifier for the images. An IP address is a numeric label assigned to a computer or digital device that is logged onto the internet. The CPS software has a single-user feature which isolates the information to one IP address containing the known hashtag for the confirmed child pornography.

Using the CPS software, the agent identified a user with the IP address 70.179.42.22 on the Gnutella network with child-pornography files available for download. The agent downloaded two files from the user. On the same day, the agent utilized an internet geo-location service available online to the public and determined that the IP address associated with the downloaded child pornography belonged to the internet service provider Cox Communications.

On January 7, 2014, the agent submitted an administrative summons to Cox Communications seeking subscriber information for the IP address 70.179.42.22. The summons stated in part: "*You are requested not to disclose the existence of this summons for an indefinite period of time. Any such disclosure will impede this investigation and thereby interfere with the enforcement of federal law.*" (ECF No. 27-3 at 3). Cox identified the subscriber of the IP address at the relevant time to be Joseph Kline, and provided the Government with an address for the subscriber. The agent obtained a search warrant authorizing the search and seizure of evidence related to child pornography offenses from the identified address.

On March 24, 2014, agents executed the warrant and seized numerous electronic devices from Defendant's residence. A forensic analysis confirmed the presence of image files and video files containing child pornography, including the pornography file downloaded by the agent at the inception of the investigation.

IP Address Information

Defendant contends that obtaining his IP address information without a warrant violated his Fourth Amendment rights under the United States Constitution. Defendant

contends that recent Supreme Court jurisprudence[6] has undermined the third-party-disclosure doctrine relied upon in prior cases which conclude that obtaining IP address information without a warrant was constitutional. The United States contends that binding authority in this circuit[7] establishes that there is no expectation of privacy in IP address information.

"[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). A Fourth Amendment search "occurs when the government violates a subjective expectation of privacy that society recognizes." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley v. California*, 134 S.Ct. at 2482. "[The Supreme] Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976) (citations omitted). In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that the use of a pen register installed on telephone company property does not constitute a search for Fourth Amendment purposes. The Supreme Court noted initially that pen registers acquire only the telephone numbers that have been dialed and "do not acquire *contents* of communications." *Id*. at 741. The Court explained, "All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment

---

[6] *Riley v. California*, _ U.S. _, 134 S. Ct. 2473 (2014), and *United States v. Jones*, _U.S. _, 132 S. Ct. 945 (2012)

[7] *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008)

that their calls are completed." *Id*. at 741. The Supreme Court "conclude[d] that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'" *Id*. at 745-46.

In *United States v. Forrester*, the Court of Appeals for the Ninth Circuit addressed the constitutionality of warrantless computer surveillance techniques which revealed to/from addresses of e-mail messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account. The Court of Appeals stated:

> We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. First, e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the 'switching equipment that processed those numbers,' e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather voluntarily turned over in order to direct the third party's servers.
>
> Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses - but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. . . . [T]he Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

512 F.3d at 510 (citations and footnote omitted).

In *United States v. Jones*, the Supreme Court held that the Government's installation of a GPS device on a target vehicle to monitor the vehicle's movement constituted a search and required a warrant. The Supreme Court found that the

"Government physically occupied private property for the purposes of obtaining information" which "would have been considered a search within the meaning of the Fourth Amendment when it was adopted." 132 S.Ct. at 949. The Supreme Court explained, "Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, . . . a search has undoubtedly occurred." *Id.* at 950 n.3.

In *Riley v. California*, the Supreme Court concluded that accessing digital data from a cell phone seized after an arrest was a search. The Supreme Court concluded that interest in protecting officer safety and preventing destruction of evidence did not justify dispensing with the warrant requirement. The Supreme Court rejected the application of *Smith v. Maryland*, explaining,

> We also reject the United States' final suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case. The Government relies on *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a 'search' at all under the Fourth Amendment. *See id.*, at 745–746, 99 S.Ct. 2577. There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label 'my house' in Wurie's case.

134 S.Ct. at 2492.

This Court concludes that the decisions in *Jones* and *Riley* do not provide a basis to reject the third party doctrine set forth in *Smith v. Maryland* and relied upon by the Court of Appeals in *Forrester*. *But see Jones*, 132 S.Ct. at 957 (Sotomayer concurring) ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."). In *Jones* and *Riley*, the Supreme Court concluded that law enforcement engaged in the search of property without an exception to the Fourth Amendment warrant requirement. In *Smith* and *Forrester*, law enforcement obtained unprotected addressing information provided to third parties "for the specific purpose of directing the routing of information." *Forrester*, 512 F.3d at 510.

In this case, the agent initiated an investigation using the CPS software program that searched for the hashtags of known child pornography available to anyone on the internet who has downloaded the peer-to-peer software on the Gnutella network. The CPS program identified files with hashtags for known child pornography from the network and provided the agent with the IP address information for those files. The files were placed in the peer-to-peer network for access by other users of the peer-to-peer network. The content of the files was not revealed by the CPS software but by the user of the peer-to-peer software program placing the files on the network for access by anyone on the internet who has also downloaded the peer-to-peer software. The CPS software revealed the numerical label assigned to the digital device providing the child pornography files. As in *Forrester*, "this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." 512 F.3d at 510. The CPS software provided "unprotected addressing information" and there was no requirement that the agent obtain a warrant. *Id.* After obtaining the IP address information, the agent used a publically available internet search program to determine that Cox Communications was the service provider for the IP address. The Court concludes that the investigation techniques employed by Agent Coderes did not require a warrant.

The motion to suppress evidence is denied**.**

Administrative summons

The administrative subpoena issued to Cox Communication ons on January 7, 2014, complied with the requirements of 18 U.S.C. § 2703(c)(2),(3). The summons issued to Cox Communications stated in relevant part: "*You are requested not to disclose the existence of this summons for an indefinite period of time. Any such disclosure will impede this investigation and thereby interfere with the enforcement of federal law.*" (ECF No. 27-3 at 3). This provision is consistent with § 2703(c)(3) ("A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."). The request to Cox

Communication not to disclose the summons to the customer does not require suppression of evidence.

IV. Conclusion

IT IS HEREBY ORDERED that the motion to dismiss information (ECF No. 27-1) is denied, and the motion to suppress fruit of unlawful search (ECF No. 27-2) is denied. IT IS FURTHER ORDERED that the motion to suppress evidence for a *Gantt* violation (ECF No. 27-3), the motion to suppress statements (ECF No. 27-4), and the motion to compel discovery (ECF No. 27-5) are denied as moot.

DATED: November 12, 2015

WILLIAM Q. HAYES
United States District Judge